Habemus Segwit

scritto da Alberto De Luigi | 24 Luglio 2017

Alle 6.46 di domenica 23 luglio, ora italiana, il blocco 477.120 della blockchain ha segnato una svolta nella storia. È stato attivato BIP91, il Bitcoin Improvement Proposal che costituisce la prima parte dell'upgrade SegWit2x.

L'inizio della segnalazione per BIP91 era previsto il 21 luglio, ma i miners hanno anticipato le votazioni, forse per impedire un aggravarsi della crisi nei mercati, turbati dal timore di un fork contenzioso. BIP91 è stato quasi un plebiscito e ha raggiunto immediatamente la soglia prevista, rivelando una community internazionale particolarmente unita.

L'esito di BIP91, ora che è attivo, è quello di orfanare tutti i blocchi che non segnalano bit 1 nel version field. Segnalare bit 1 significa votare per l'upgrade Segregated Witness (BIP141). Perciò, qualsiasi miner che oggi creasse ancora blocchi senza bit 1, li vedrebbe rifiutati dalla quasi totalità del network e si ritroverebbe così in un fork della blockchain, con una moneta senza valore. Nessun miner avrebbe convenienza a farlo, poiché pagherebbe energia elettrica per effettuare calcoli, senza in cambio ottenere una moneta che

sia spendibile e accettata dalla community.
Dal momento che oggi il 100% sta votando SegWit sul bit 1, il lockin di SegWit avverrà presumibilmente al blocco 479.808. Dal lockin all'attivazione ci sarà uno scarto temporale, per permettere a tutti di aggiornare il software. Se i calcoli sono corretti, dal blocco 481.824 SegWit sarà attivo, quindi il 24 agosto.

12.960 blocchi dopo l'attivazione di SegWit è prevista la seconda e ultima fase dell'upgrade SegWit2x, ovvero la creazione del "Blocco X": il blocco necessariamente più grande di 1mb, che quindi sarà il n. 494.784, il 22 novembre.

La speranza dopo SegWit è che la rete Lightning Network si sviluppi al più presto, non rendendo più necessario un aumento ulteriore della capacità dei blocchi. Qualora entro novembre non si arrivi all'esito sperato, il raddoppio della capacità onchain dovrebbe, almeno nell'intento, scongiurare l'intasamento della rete e una nuova escalation dei costi di transazione (le commissioni pagate ai miners), dando più tempo alla rete LN di diffondersi.

A novembre ci sarà quindi un raddoppio del blocksize da 1 a 2mb. Si moltiplicherà per 2 l'effetto SegWit, portando il blockweight a un tetto massimo di 8mb (anziché 4mb). Secondo alcune stime, l'effettivo peso dei pacchetti dati scambiati ogni 10 minuti con SegWit (dal 24 agosto) sarà di 1.7-2.2mb, mentre dopo l'hard fork di novembre (SegWit2x) sarà il doppio, ovvero circa 3.6-4.4mb.

Il primo agosto UASF non avrà effetto, poiché il 100% dei miner già segnala bit 1. Ogni eventualità catastrofica è stata quindi scongiurata. Ci sarà però un altro evento interessante per tutti i possessori di Bitcoin. Alcuni big blockers contrari allo scaling offchain, creeranno una nuova moneta, BitcoinCash: un hard fork di Bitcoin che dà intenzionalmente vita a una moneta separata. BitcoinCash condividerà la stessa storia di Bitcoin, ovvero la stessa blockchain fino alla

biforcazione del 1 agosto, perciò, ogni utente che sia in possesso di bitcoin e ne custodisca le chiavi private, avrà un equivalente ammontare in bitcoincash. I bitcoincash potranno essere custoditi o anche venduti immediatamente sulle piattaforme che ne permettono il cambio. È questa una buona occasione per farsi il proprio "wallet", anziché affidare a terzi la custodia dei bitcoin, come exchanges o wallets tipo Coinbase o Blockchain.info. Finché non si è in possesso delle proprie chiavi (o del seed che le genera) non si possiedono veramente bitcoin.
Ognuno è libero di adottare la strategia che preferisce, io personalmente tenterò di vendere subito i bitcoincash, sempre che al momento del fork abbiano ancora un valore di mercato significativo (e se troverò un acquirente o una piattaforma affidabile su cui sia possibile tradarli).

Ci sono criticità per il futuro di Bitcoin?
La speranza è che Lightning Network risolva al più presto (e definitivamente) i problemi di scalabilità, ma cosa accadrebbe se non li risolvesse in tempi ragionevoli? Arriveremmo a una nuova escalation delle commissioni e una rete lenta e intasata? I timori della community di ricadere in una situazione simile sono fra le motivazioni principali che spingono all'attuazione della seconda parte dell'upgrade SegWit2x, prevista a novembre.

Dall'altro lato però, l'hard fork di novembre, con la creazione del primo blocco superiore a 1mb, non piacerà a tutti. Infatti creerà un "precedente" che, secondo le visioni più intransigenti, verrà sfruttato in futuro, per ulteriori aumenti della dimensione del blocco tali da condurre all'inevitabile accentramento della rete.

I miners sembrano molto compatti nell'intenzione di portare avanti anche la seconda parte di SegWit2x, infatti ancora l'85% dei blocchi riporta la sigla "NYA" (New York Agreement) nel testo del coinbase. Questo significa che l'85% dell'hashpower segnala di essere ancora fedele all'accordo di

New York e di conseguenza è probabile che l’upgrade 2x verrà effettuato; tuttavia, questa volta potrebbe non andare tutto liscio come nel caso di SegWit. Ci saranno utenti, sviluppatori e aziende che vorranno forkare dal nework come oggi stanno facendo i promotori di BitcoinCash? Data l’assenza di una forza economica e di hashpower che lo sostiene, BitcoinCash non è visto come un problema e come un concorrente pericoloso per Bitcoin, né sembra pretendere di sostituirsi ad esso. Si potrà dire lo stesso a novembre?

Per ora, mettiamo da parte le paure e festeggiamo. Con SegWit si sono spalancate le porte all’innovazione. Ora esiste una soluzione per rendere il Bitcoin scalabile, al punto da poter servire i bisogni degli utenti anche in caso di vera adozione di massa, rimpiazzando i più comuni sistemi di pagamento attuali. Non c’è più nessuna barriera tecnologica che possa fermare la corsa del Bitcoin alla conquista della terra e… to the moon!